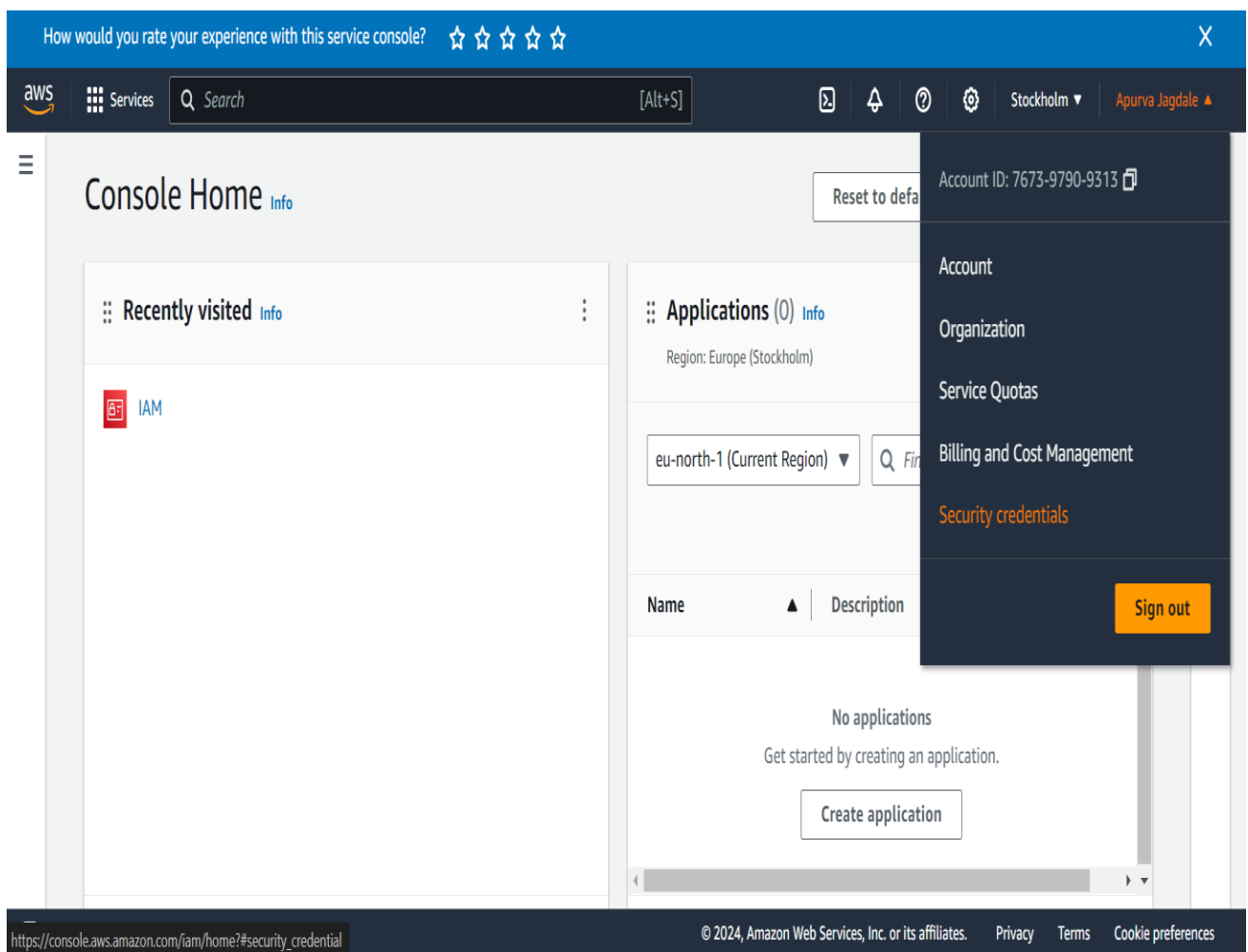


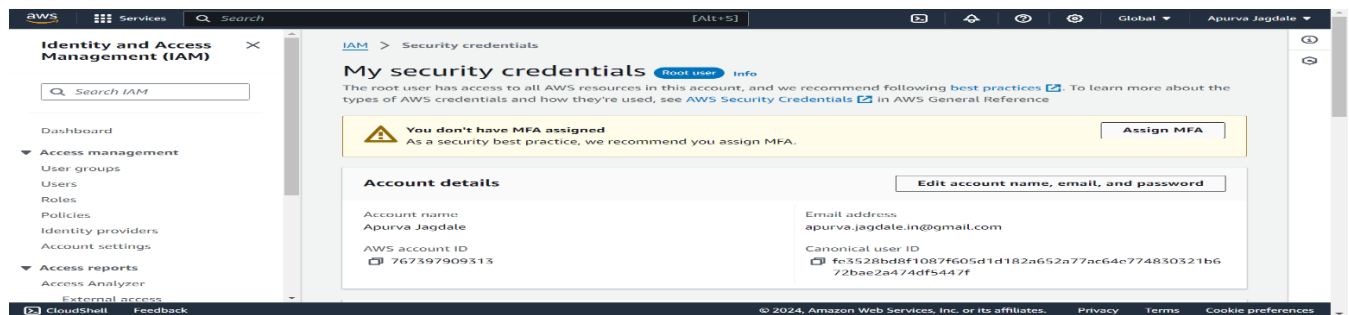
# HOW TO THE ACTIVATE AND DEACTIVATE MFA TO ROOT USER.

=> Basically, MFA code provides more Security for user.

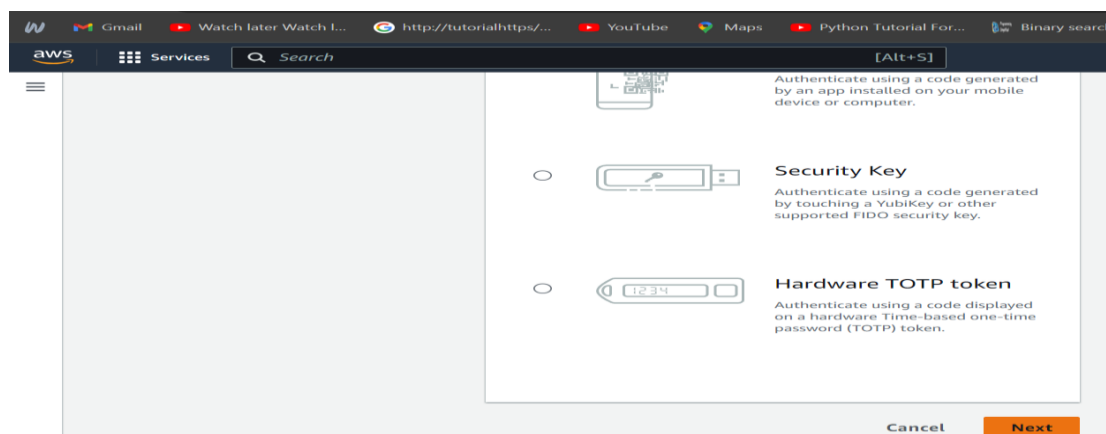
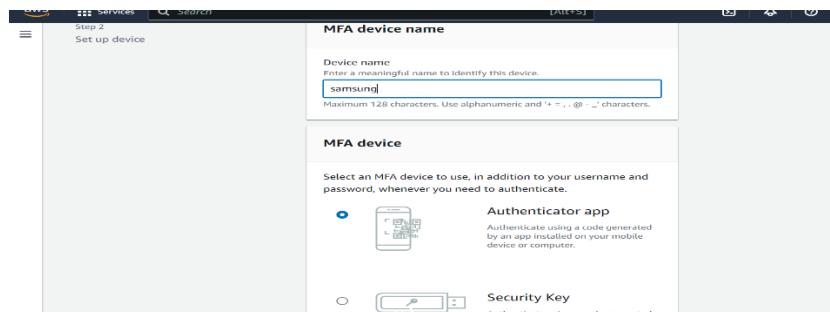
Step1: Login the AWS account using username and password. Then go to account and click on Security Credentials.



Step 2: Then click on assign MFA to root user.



Step 3: Then enter the meaningful MFA device name to identify device and also select MFA device. Then click on next



Step 4: Then using your phone and download the authenticator app using play store on your mobile phone scan this QR and get the two consecutive MFA

code type here quickly otherwise they expired new once are genetated.

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.  
[See a list of compatible applications](#)
- 2 [Show QR code](#)  
Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code.  
Alternatively, you can type a secret key. [Show secret key](#)
- 3 Fill in two consecutive codes from your MFA device.  
MFA code 1

Step 5: and get the two consecutive MFA code type here quickly otherwise they expired new once are genetated

Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2

[Show QR code](#)  
Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code.  
Alternatively, you can type a secret key. [Show secret key](#)

[See a list of compatible applications](#)

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

2

3

Cancel Previous Add MFA

Step 6: and get the two consecutive MFA code type here quickly otherwise they expired new once are generated and then click on add MFA.

✓ **MFA device assigned**

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

### Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

	Device type	Identifier	Certifications	Created on
<input type="radio"/>	Virtual	arn:aws:iam::767397909313:mfa/qwe	Not Applicable	Now

### Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Access key ID	Created on	Access key last used	Region last used	Service last used	Status
No access keys					

Step 7: MFA device assigned .then simply click on Sign out.

Account ID: 7673-9790-9313

- Account
- Organization
- Service Quotas
- Billing and Cost Management
- Security credentials

Sign out

✓ **MFA device assigned**

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

### Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

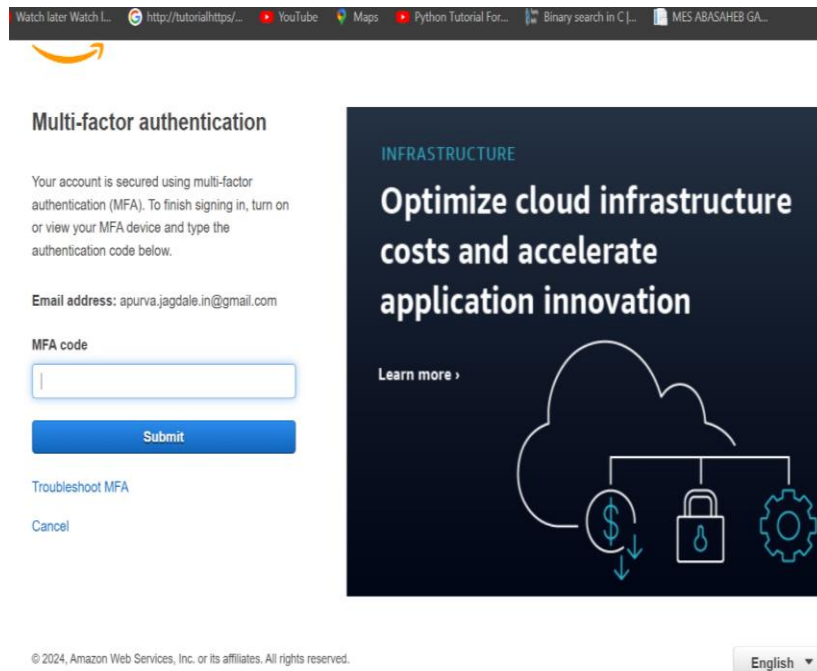
	Device type	Identifier	Certifications
<input type="radio"/>	Virtual	arn:aws:iam::767397909313:mfa/qwe	Not Applicable

### Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Create access key

Step 8: Again Login using your username and password and also asked for MFA code using authenticator app type here MFA codemit.



Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: apurva.jagdale.in@gmail.com

MFA code

Submit

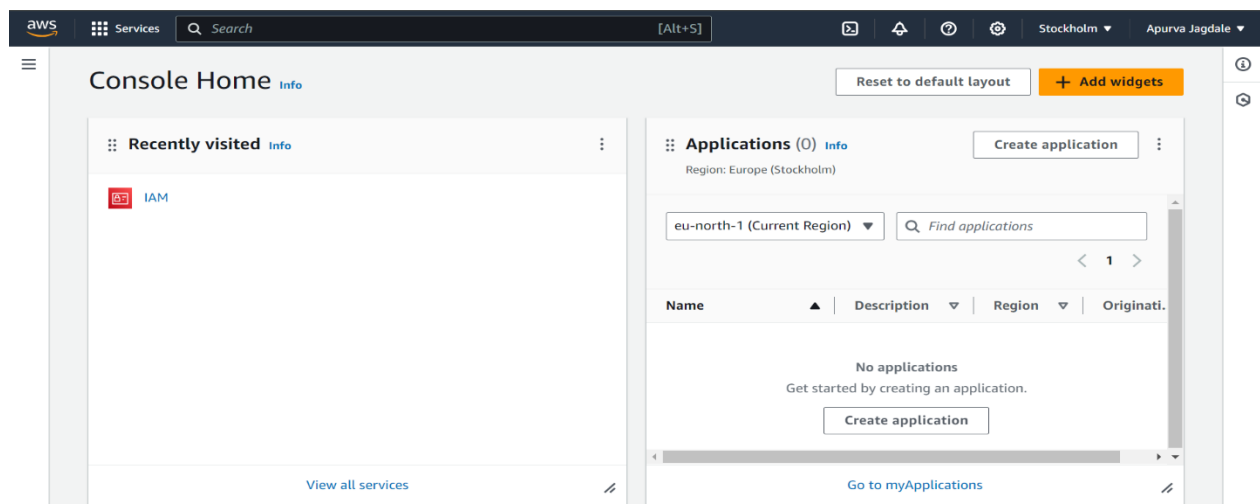
[Troubleshoot MFA](#)

[Cancel](#)

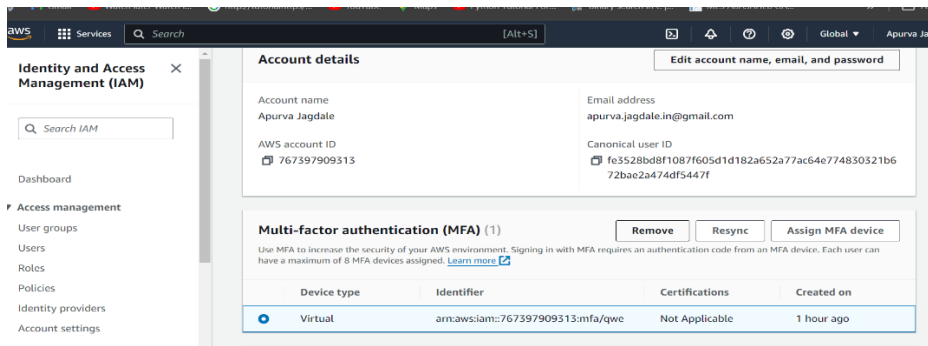
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English

And console home is open.



TO remove MFA code simply go to Security credentials and click on these MFA which we want to remove and simply click on remove button.



## Management (IAM)

Dashboard

### Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

### Access reports

Access Analytics

## My security credentials Root user Info

The root user has access to all AWS resources in this account, and we recommend following best practices for types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.



### You don't have MFA assigned

As a security best practice, we recommend you assign MFA.

### Account details

Edit account details

Account name

Apurva Jagdale

AWS account ID

767397909313

Email address

apurva.jagdale.in@gmail.com

Canonical user ID

fe3528bd8f1087f605d1d182a652a77ac64e774830321b672bae2a474df5447f

See here MFA device is deleted now.

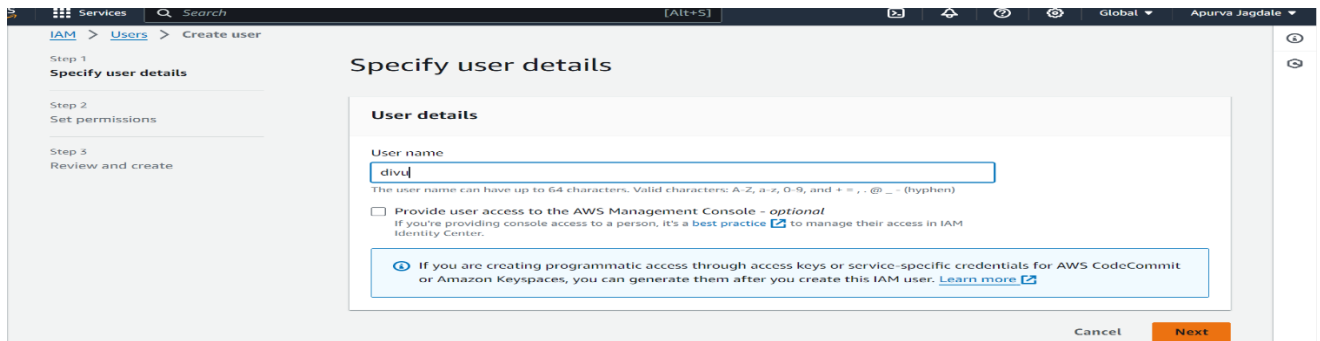
# HOW TO CREATE IAM USER ?

Step 1 : Login your account using root user then search in service IAM service click on it .

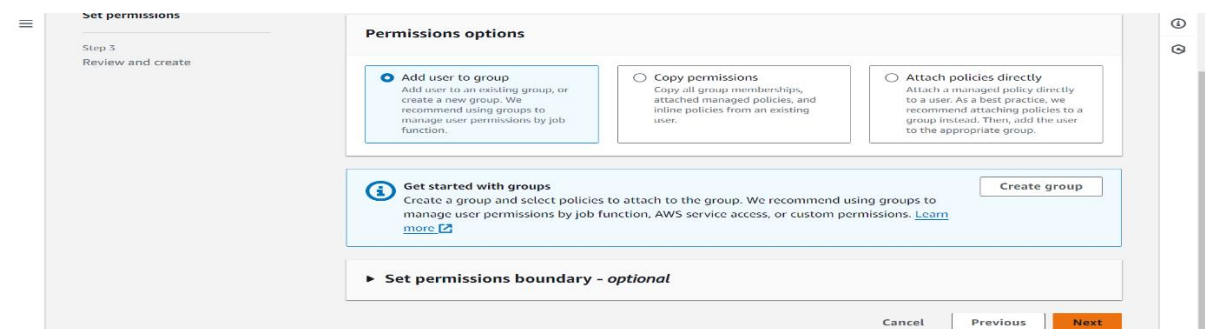
Step 2 :Then In access management click on users and then click on create user.



Step 3: then Specify here user details as a username then click on next button.



Step 4:set the permissions here it is optional then click on next button.



Step 5: Review it and click on create user.

Permissions summary < 1 >

Name	Type	Used as
No resources		

**Tags - optional**  
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)  
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

Step 6: and finally we get the pop up user created successfully.

**User created successfully**  
You can view and download the user's password and email instructions for signing in to the AWS Management Console. [View user](#)

[IAM](#) > Users

**Users (2)** [Info](#) [Refresh](#) [Delete](#) [Create user](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password
<input type="checkbox"/>	<a href="#">divu</a>	/	o		-	-
<input type="checkbox"/>	<a href="#">raavi</a>	/	o		-	<a href="#">View</a> 4

TASK 3:ASSIGN THE CUSTOM PASSWORD TO USER.

Step 1: Login your account using root user then search in service IAM service click on it .

Search results for 'iam'

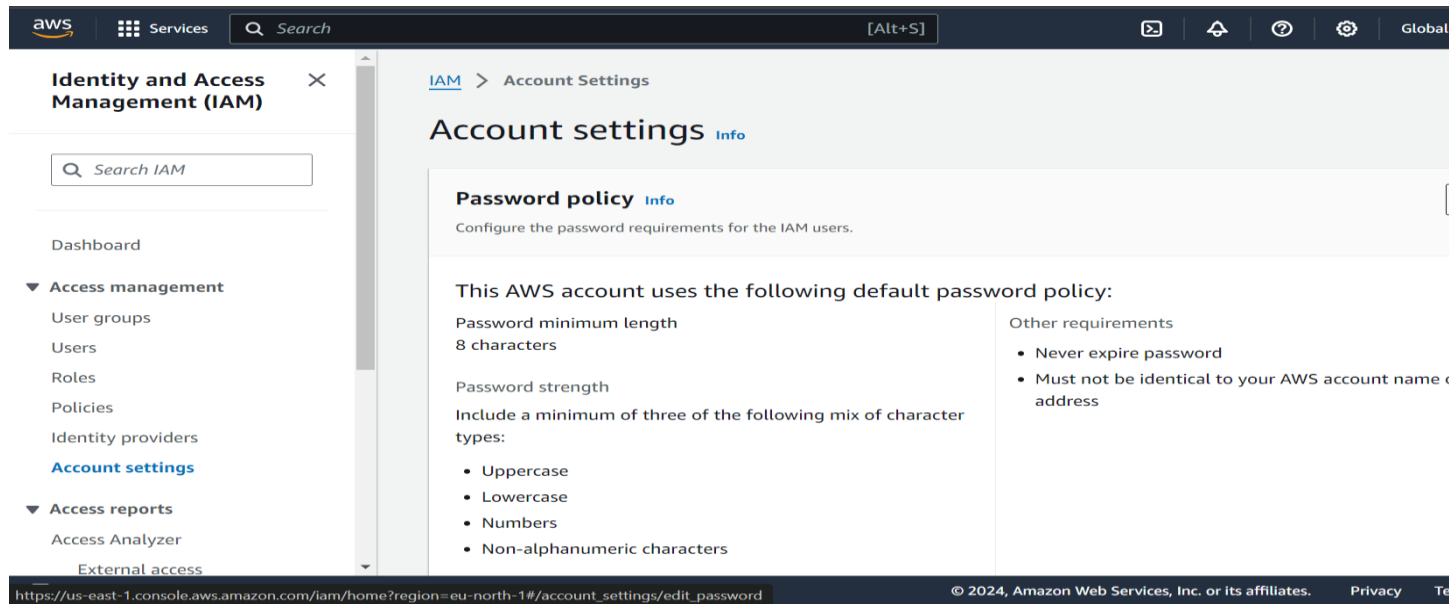
**Services (11)** [See all 11 results](#)

- IAM** [Star](#)  
Manage access to AWS resources
- IAM Identity Center** [Star](#)  
Manage workforce user access to multiple AWS accounts and cloud applications
- Resource Access Manager** [Star](#)  
Share AWS resources with other accounts or AWS Organizations
- AWS App Mesh** [Star](#)  
Easily monitor and control microservices

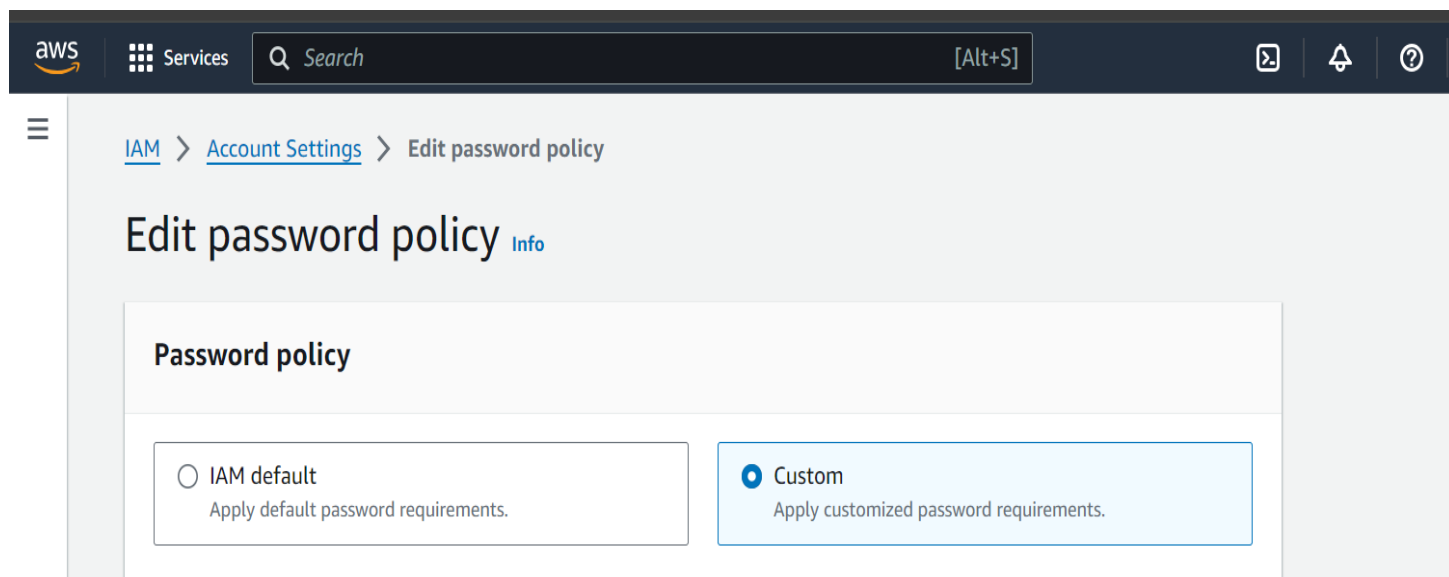
**Features (22)** [See all 22 results](#)



Step 2: In access Management click on account Settings and then click on edit option .



Step 3: In Password Policy, we have customized the password so select Custom Option



Step 4: Select the option as per requirements and click on the Save changes option.

7 characters  
Needs to be between 6 and 128.

**Password strength**

- ☒ Require at least one uppercase letter from the Latin alphabet (A-Z)
- ☒ Require at least one lowercase letter from the Latin alphabet (a-z)
- ☒ Require at least one number
- ☒ Require at least one non-alphanumeric character ( ! @ # \$ % ^ & \* ( ) \_ + - = [ ] | ' )

**Other requirements**

- ☒ Turn on password expiration
  - Expire password in 13 day(s)  
Needs to be between 1 and 1095 days.
- ☒ Password expiration requires administrator reset
- ☒ Allow users to change their own password
- ☒ Prevent password reuse
  - Remember 5 password(s)  
Needs to be between 1 and 24.

Cancel Save changes

Step 5 : the click on these set custom

## Set custom password policy?

This will impact any new user creation and all the existing users changing passwords.

Cancel

Step 6: And Finally Password requirements for IAM users are updated these Pop-up is generated.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access

Password requirements for IAM users are updated.

### Account settings

**Password policy**

Configure the password requirements for the IAM users.

This AWS account uses the following custom password policy:

**Password minimum length**

7 characters

**Password strength**

- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character

**Other requirements**

- Password expires in 13 day(s)
- Password expiration requires administrator reset
- Allow users to change their own password
- Prevent password reuse from the past 5 changes

Edit